REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 22-05-2015	2. REPORT TYPE Final Report	3. DATES COVERED (From - To) 24-Feb-2012 - 23-Feb-2015

4. TITLE AND SUBTITLE
Final Report: Trusted Module Acquisition Through Proof-Carrying Hardware Intellectual Property

5a. CONTRACT NUMBER
W911NF-12-1-0091

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
Yiorgos Makris

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Texas at Dallas
800 West Campbell Road, AD15

Richardson, TX 75080 -3021

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
60709-CS.7

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

By borrowing ideas from the proof carrying code (PCC) in software domain, in this project we introduced the proof carrying hardware intellectual property (PCHIP) framework, which aims to ensure the trustworthiness of third-party hardware IPs utilizing formal methods. We were able to build the fundamental PCHIP framework, enhance its capabilities to be usable for various hardware types with different requirements, e.g. microprocessor IPs or cryptographic cores, and automate parts or all of the extra duties imposed by the PCHIP on hardware IP developers. PCHIP involves these three additional tasks: development of security properties for the design as formal theorems

15. SUBJECT TERMS
Proof Carrying Hardware, Hardware Security, Third-Party Intellectual Property, Verification

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Yiorgos Makris
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU	UU		19b. TELEPHONE NUMBER 972-883-2910

Report Title

Final Report: Trusted Module Acquisition Through Proof-Carrying Hardware Intellectual Property

ABSTRACT

By borrowing ideas from the proof carrying code (PCC) in software domain, in this project we introduced the proof carrying hardware intellectual property (PCHIP) framework, which aims to ensure the trustworthiness of third-party hardware IPs utilizing formal methods. We were able to build the fundamental PCHIP framework, enhance its capabilities to be usable for various hardware types with different requirements, e.g. microprocessor IPs or cryptographic cores, and automate parts or all of the extra duties imposed by the PCHIP on hardware IP developers. PCHIP involves these three additional tasks: development of security properties for the design as formal theorems, conversion of the HDL code to the formal representation, and construction of formal proofs for those security theorems. We established a set of security properties which ensure the trustworthiness of microprocessor IPs and developed VeriCoq, which automates the conversion of hardware IPs in Verilog to their equivalent Coq representation. We also built a special PCHIP framework for cryptographic cores, capable of tracking sensitive information through the design and ensure their secureness. Finally, we developed VeriCoq-IFT, which automates all of PCHIP's tasks for this special framework, including conversion of HDL code to formal representation and generation of security theorems and their proofs.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

05/20/2015 5.00 Mohammad-Mahdi Bidmeshki, Yiorgos Makris. VeriCoq: A Verilog-to-Coq Converter forProof-Carrying Hardware Automation,
IEEE International Symposium on Circuits and Systems. 25-MAY-15, . : ,

05/20/2015 6.00 Mohammad-Mahdi Bidmeshki, Yiorgos Makris. Toward Automatic Proof Generation for InformationFlow Policies in Third-Party Hardware IP,
IEEE Hardware Oriented Security and Trust Symposium. 06-MAY-15, . : ,

08/29/2014 4.00 Yier Jin, Yiorgos Makris. A proof-carrying based framework for trusted microprocessor IP,
2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). 17-NOV-13, San Jose, CA, USA. : ,

08/30/2013 2.00 Bo Yang, Yiorgos Makris, Yier Jin. Cycle-accurate information assurance by proof-carrying based signal sensitivity tracing,
2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). 01-JUN-13, Austin, TX, USA. : ,

08/30/2013 3.00 Nagmeh Karimi, Jayevijendran. Rajendran , Ramesh Karri, Yier Jin, Ke Huang, Yiorgos Makris, Ozgur Sinanoglu. Reconciling the IC Test and Security Dichotomy,
IEEE European Test Symposium. 27-MAY-13, . : ,

08/31/2012 1.00 Yier Jin, Yiorgos Makris. Proof Carrying-Based Information Flow Tracking for Data Secrecy Protection and Hardware Trust,
IEEE VLSI Test Symposium. 24-APR-12, . : ,

TOTAL: **6**

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received	Paper

TOTAL:

Number of Manuscripts:

Books

Received	Book

TOTAL:

Received	Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Mohammad-Mahdi Bidmeshki	1.00	
FTE Equivalent:	**1.00**	
Total Number:	**1**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Yiorgos Makris	0.04	No
FTE Equivalent:	**0.04**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:...... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):...... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:...... 0.00

Names of Personnel receiving masters degrees

NAME	
Tianyu Chen	
Total Number:	**1**

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

See Attachment

Technology Transfer

SCIENTIFIC PROGRESS FOR
ARO 60709-CS: 08/01/14 – 01/31/15

Yiorgos Makris, Professor
Electrical Engineering Department, University of Texas at Dallas
(yiorgos.makris@utdallas.edu)

Summary of Key Technical Developments

The key new piece added in this reporting period is the implementation and complete development of the automated framework we described for the Proof-Carrying Hardware IP (PCHIP) methodology in the previous report. Although PCHIP is extremely effective in preventing hardware Trojans to sneak into the final product through third party hardware IPs, it comprises the onerous task of converting a design to a formal representation and developing proofs for the desired security properties and thus requires extra knowledge of formal reasoning methods, proof development and proof checking. To make PCHIP more striking, we pursued automation in several aspects of the PCHIP framework. As the first step towards the automation of PCHIP, we examined and improved the conversion rules from HDL to Coq formal representation and developed an automatic convertor named Vericoq [1] to convert the exact circuit functionality and structure into the Coq formal representation. Vericoq makes the conversion process of the HDL code to the Coq formal representation automatic and straight forward, and creates the basis for our PCHIP automation framework. However, development of security properties stated as theorems in Coq and construction of proofs for such theorems still remains in the responsibility of the IP developer and still requires extra effort and knowledge. In an effort to automate the whole process, we focused on the enforcement of information flow policies as we presented earlier in [2, 3], which is mainly applicable to capture sensitive information leakage in cryptographic hardware cores through design flaws or malicious capabilities. We developed VeriCoq-IFT [4] to automate all the extra tasks required in the PCHIP methodology for information flow policies. In addition to automating the conversion of the HDL code to the Coq formal representation, VeriCoq-IFT automatically generates security property theorems to ensure information flow policies, constructs proofs for such theorems and checks their validity for the design with minimal user intervention. We successfully tested this automated framework by utilizing it to evaluate the trustworthiness of several genuine and Trojan infested DES and AES cryptographic cores.

VeriCoq: Automated Verilog to Coq Converter

In the previous reporting periods of this project we demonstrated our framework for hardware IP protection called proof carrying hardware intellectual property (PCHIP) as depicted in Figure 1. In this framework, hardware IP developers are required to deliver formal proofs of a set of security properties for the design along with the HDL code. These security properties are crafted in a way that prevent malicious activities in the hardware IP, are specific to the design, and are stated as formal theorems in Coq. Coq allows development and mechanized checking of the proofs of these formal security property theorems, and thus enables the trustworthiness assessment of the design in terms of these security properties. To be able to develop the proofs of the security properties for the design, the hardware IP should also be described formally in Coq. For this purpose, PCHIP defines rules to convert the design HDL to its equivalent Coq representation. To make this conversion task easier, we revised and augmented the PCHIP conversion rules and developed Vericoq [1], an automatic Verilog to Coq converter which precisely converts the circuit structure and functionality to the equivalent Coq representation. Vericoq supports almost every synthesizable statement in Verilog and can manage arrays, parameters and hierarchical module structures. It converts a design in Verilog into Coq representation with minimal user involvement. In [5] we showed how such rules and conversion helps to ensure the trustworthiness of microprocessor IPs through proof checking of the appropriate security properties. As Figure 1 shows, VeriCoq helps both IP developers and IP consumers in PCHIP framework. IP developers utilize VeriCoq to convert the HDL code to the Coq representation and develop the proofs of security properties. On the other hand, IP consumers use VeriCoq when checking the validity of the proofs for the hardware design.

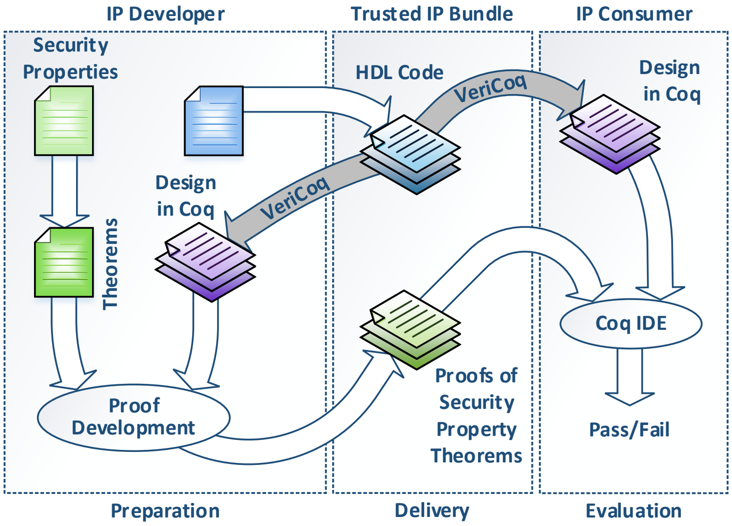

Figure 1. PCHIP framework and VeriCoq application

Automated PCHIP Framework for Information Flow Policies

Developing security properties to ensure the hardware IP trustworthiness and constructing proofs for them is generally specific to each design and there is a narrow room for the automation of this task. Information flow policies stated as security property theorems are a set of policies which ensure that no secret information is leaked through untrusted channels and are mainly applicable to cryptographic circuits and designs which manipulate secret and sensitive data. Earlier in [2, 3] we demonstrated enforcing such policies to ensure the trustworthiness of cryptographic hardware for DES and AES cores. Information flow policies allow to develop a common structure in which most of security property theorems and their proofs can be constructed automatically. Normally, information flow policies are not concerned about the exact functionality of the circuit and type of operations. Instead, they usually define policies regarding to the interaction of information in the design. Therefore, we revised the rules to convert Verilog design to Coq representation specifically to enforce information flow policies. While these rules are comprehensive enough to support common statements and structures used in circuit description, they are narrow enough which allow the automation of security property theorems generation and proof construction. For this purpose, developed Vericoq-IFT [4] as depicted in Figure 2, which aims to (i) automate the process of converting designs from HDL to the Coq formal language to evaluate information flow policies, (ii) generate security property theorems ensuring information flow policies, (iii) construct proofs for such theorems, and (iv) check their validity for the design, with minimal user intervention. To facilitate the process, Vericoq-IFT gathers necessary information, such as the sensitivity level of the signals in the design or the declassification operations through special comments (pragmas) in the HDL code. Thus, the hardware IP developer does not need anything more than simply inserting appropriate comments in the HDL code. Vericoq-IFT also analyzes the HDL code and generates the appropriate theorems to enforce information flow policies. We also developed various lemmas used to prove the information flow policy theorems. Therefore, VeriCoq-IFT is able to generate the proof of those theorems for the design without user intervention. As Figure 2 shows, all tasks involve in the PCHIP for information flow policies are automated by VeriCoq-IFT framework.

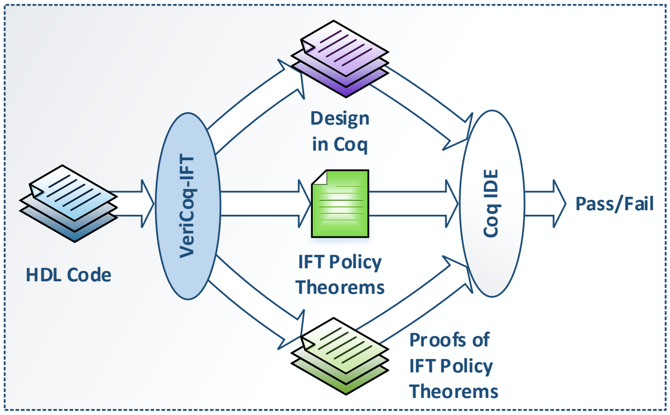

Figure 2. VeriCoq-IFT framework

To utilize VeriCoq-IFT to ensure the trustworthiness of hardware IPs in terms of the information flow policies, IP consumers first need to verify the authenticity of the special comments (pragmas) which are inserted by the IP developers into the HDL code to define the sensitivity levels of the signals and declassifying operations for VeriCoq-IFT. Then, IP consumers provide the HDL code to VeriCoq-IFT to get the design in Coq representation, IFT policy theorems and their proofs. By providing these essential pieces to the Coq IDE, IP consumers can seamlessly verify the proofs and evaluate the design trustworthiness.

VeriCoq-IFT in Action

We utilized VeriCoq-IFT to evaluate the trustworthiness of several genuine and Trojan infested cryptographic cores. These evaluations show the effectiveness of VeriCoq-IFT and its capabilities in handling various designs, with varied complexities. We consider two different implementations of DES, which is a relatively simple cryptographic algorithm as shown in Figure 3. It comprises of 16 similar rounds, preceded and succeeded by permutation steps. The area efficient DES core we evaluated implements only a single round of the encryption. Therefore, the complete encryption requires to be done in 16 iterations. Although this design is genuine, the proof of the information flow policy theorems fails for this design. Since the permutation is deterministic, there exists a potential information leakage path for this design in the first round which is marked in Figure 3 and is captured by the VeriCoq-IFT framework. We also evaluated another high performance DES core which is a pipeline design in 16 stages. The Proofs for this high performance DES core are verified in Coq, meaning its compliance with the information flow policies.

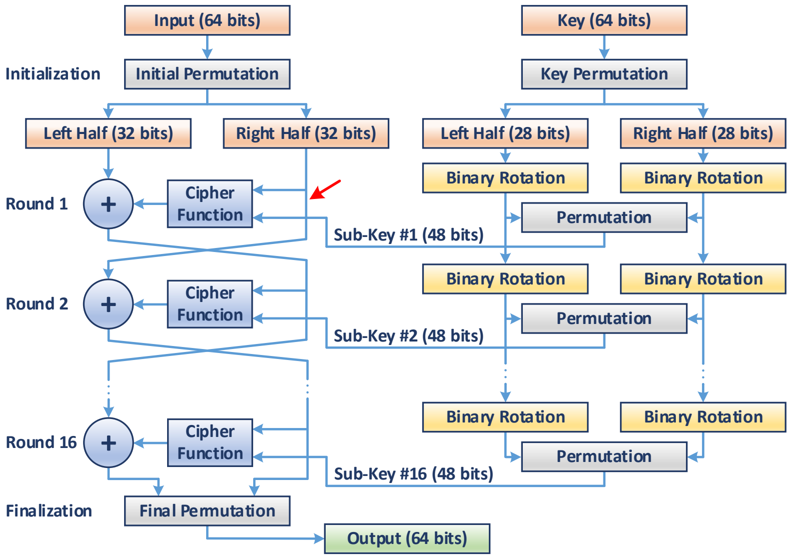

Figure 3. DES block diagram

We also evaluated a genuine and several Trojan infested 128 bits AES cores. AES is a more complex encryption algorithm compared to the DES and comprises of 10 encryption rounds. Evaluation of the genuine AES core is successful and the proofs are verified in Coq.

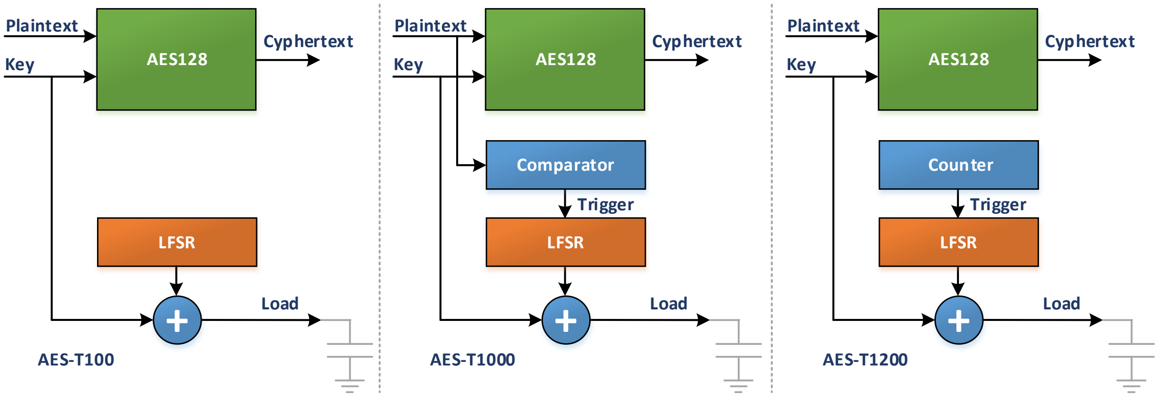

Figure 4. Three Trojan infested AES designs evaluated by VeriCoq-IFT

To have further evaluations, we considered 3 Trojan infested AES designs from trust-hub website [6] as shown in Figure 4. These Trojans try to leak 8 bits of the key through a covert channel by a CDMA like modulation. Although the leaking mechanism is similar for these Trojans, they have different triggers. AES-T100 is always active, AES-T1000 is triggered by a predefined plaintext input, while AES-T1200 is activated after a predefined number of encryptions. Proofs of information flow policies fails for these Trojan infested designs and VeriCoq-IFT successfully captures possible information leakage channels.

Progress vs. Proposed Plan of Activities

Figure 5 shows the three-year plan for this ARO-sponsored project. In the end of the third year, we have prepared and developed all of what has been projected through the end of the project. We implemented Vericoq as an automatic Verilog to Coq converter to acquire the exact circuit functionality and structure in Coq. It automates part of the PCHIP methodology and helps the developers to focus on the definition of security properties and construction of their proofs. Enforcing information flow policies for DES and AES circuits has been earlier presented in [2, 3] which we revised and improved for Vericoq-IFT development. Vericoq-IFT automates the whole process of enforcing information flow policies including Verilog to Coq conversion, security theorems generation, proof construction and verification.

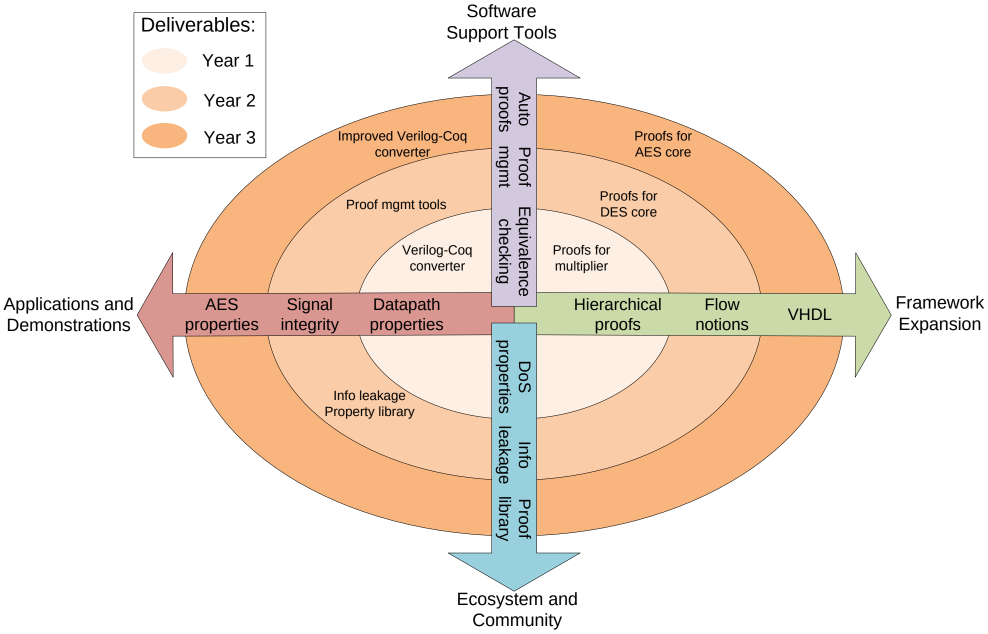

Figure 5. Overview of planned activities in the ARO-sponsored project

References

[1] M.-M. Bidmeshki and Y. Makris, “VeriCoq: A Verilog-to-Coq converter for proof-carrying hardware automation,” in *Int. Symp. Circuits and Systems*. IEEE, 2015.

[2] Y. Jin and Y. Makris, “Proof carrying-based information flow tracking for data secrecy protection and hardware trust,” in *Proc. IEEE VLSI Test Symposium*, 2012, pp. 252–257.

[3] Y. Jin, B. Yang, and Y. Makris, “Cycle-accurate information assurance by proof-carrying based signal sensitivity tracing,” in *Int. Symp. Hardware-Oriented Security and Trust*. IEEE, 2013, pp. 99–106.

[4] M.-M. Bidmeshki and Y. Makris, “Toward automatic proof generation for information flow policies in third-party hardware IP,” in *Int. Symp. Hardware-Oriented Security and Trust*. IEEE, 2015, pp. 163–168.

[5] Y. Jin and Y. Makris, “A proof-carrying based framework for trusted microprocessor IP,” in *Proc. IEEE/ACM Int. Conf. Computer-Aided Design*, 2013, pp. 824–829.

[6] Trust-Hub. [Online]. Available: https://www.trust-hub.org/